SECURITY ANALYSIS AND IMPROVEMENT OF DEFI PROTOCOLS

Bc. Adam Šmehýl

Supervisor: doc. Ing. Ivan Homoliak, Ph.D.

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2026

Motivation

Frequent exploits and scams in DeFi keep users highly sensitive to security risk, leading them to favor long-established protocols with stronger security track records.
This preference concentrates capital in legacy protocols whose design models are not always well-suited to deploying large volumes of capital efficiently. As a result, a meaningful share of managed capital remains idle or earns below 5% APY.

Research Questions

- How can idle capital in DeFi protocols be utilized more efficiently?
- Can this be achieved by extending existing protocols?

This work proposes two improvements aimed at increasing capital efficiency in DeFi protocols.

Idle Capital Allocation

Pool-based lending relies on reserve overprovisioning, which leaves a share of supplied capital idle. The proposed extension deploys that inactive capital into an external yield source.

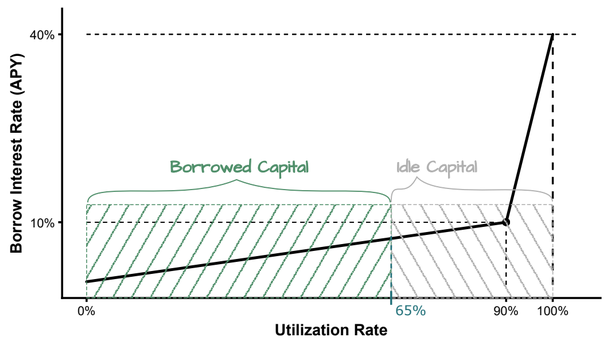


Figure 1: Illustration of capital split in a lending pool at 65% utilization, where borrowed capital earns interest while the remaining share stays idle.

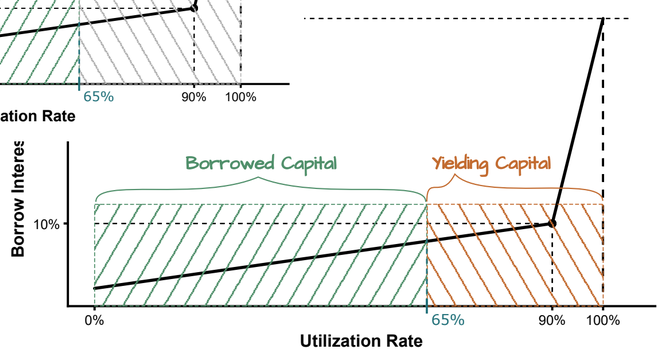


Figure 2: Reallocation of idle pool capital into an external yield strategy under the same 65% utilization scenario.

Yield Effect

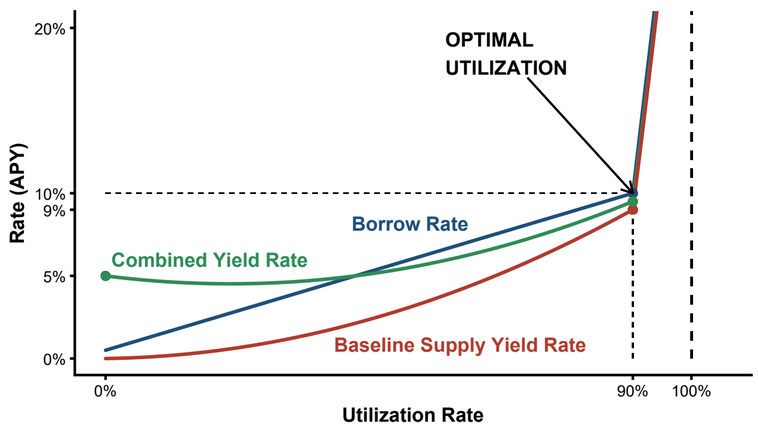


Figure 3: Comparison of borrow rate, baseline supply yield, and combined supplier yield, showing how external allocation of idle capital can lift supplier returns above the pool-only baseline.

Extension-Based Architecture

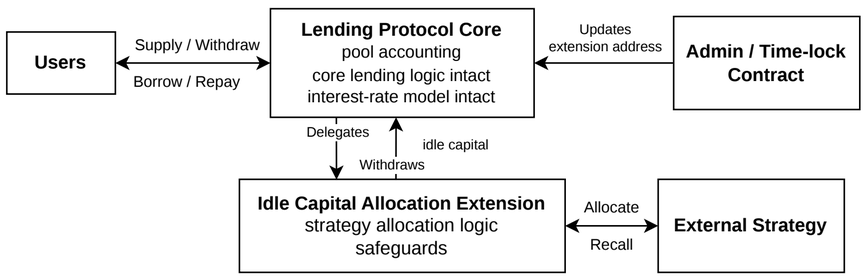


Figure 4: Extension-based architecture for idle-capital allocation, preserving core lending logic while delegating external deployment to a separate module.

Expected Supplier APY Increase

Table 1: Absolute increase in supplier APY, in percentage points, resulting from external deployment of idle pool capital under selected utilization levels and external strategy yields.

Ext. APY	Pool utilization								
	10%	20%	30%	40%	50%	60%	70%	80%	90%
2%	1.8	1.6	1.4	1.2	1.0	0.8	0.6	0.4	0.2
3%	2.7	2.4	2.1	1.8	1.5	1.2	0.9	0.6	0.3
4%	3.6	3.2	2.8	2.4	2.0	1.6	1.2	0.8	0.4
5%	4.5	4.0	3.5	3.0	2.5	2.0	1.5	1.0	0.5
7%	6.3	5.6	4.9	4.2	3.5	2.8	2.1	1.4	0.7
10%	9.0	8.0	7.0	6.0	5.0	4.0	3.0	2.0	1.0

The proposed extension improves supplier-side capital efficiency while preserving the baseline behavior of the lending protocol.

Automated Liquidity Position Range Migration

Because narrow concentrated-liquidity positions can be pushed out of the allocated price range by persistent directional drift, the proposed mechanism aims to automatically migrate the position range to preserve active exposure.

Directional Drift Problem

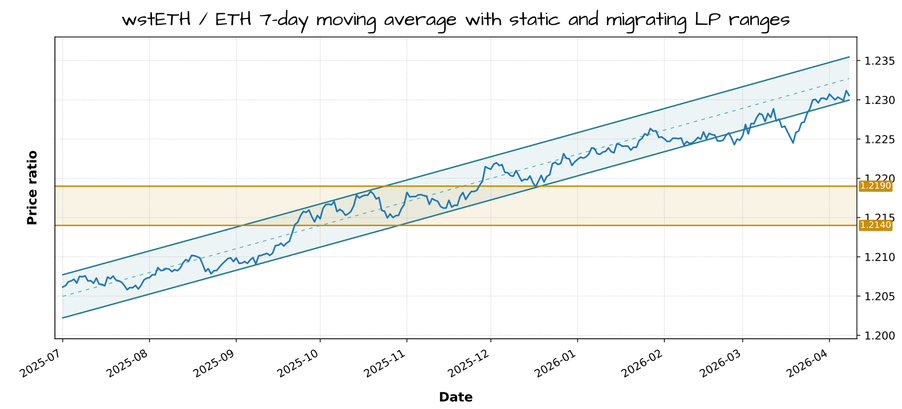


Figure 5: Price-ratio development of the wstETH/ETH pair with example static and migrating liquidity ranges, showing how directional drift can push narrow positions out of range.

Range Migration Mechanism

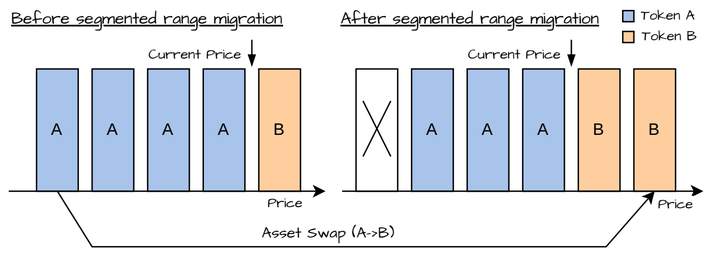
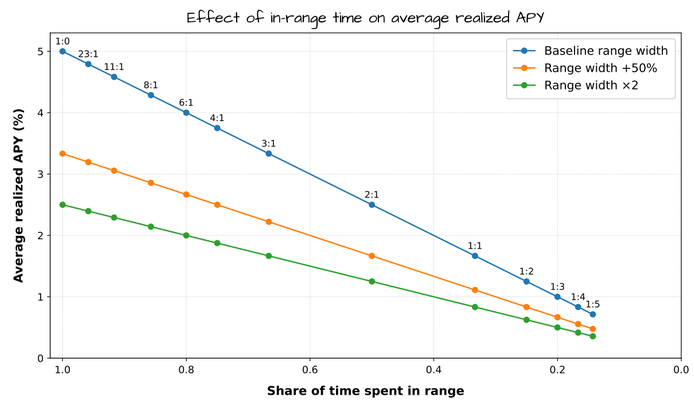


Figure 6: Segmented range migration in a concentrated-liquidity position, showing withdrawal of trailing liquidity and reallocation on the advancing side.

Evaluation Context

Figure 7: Illustrative trade-off between realized APY and time spent in range for concentrated-liquidity positions with different static range widths, showing that narrower ranges can deliver higher peak efficiency but are more sensitive to out-of-range exposure.



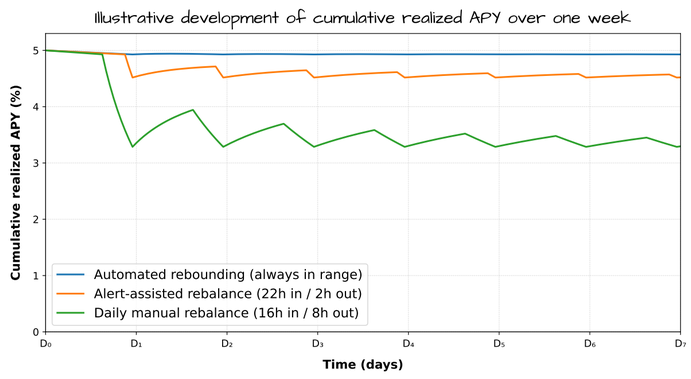


Figure 8: Prototype comparison of cumulative realized position APY over one week under automated range migration and two manual repositioning schedules.

The economic effect of this mechanism is difficult to assess in absolute terms because realized performance depends on future price development, trading activity, and execution costs.

Discussion

- Although both improvements are conceptually simple, they remain largely underexplored in current DeFi protocols.
- Since both proposals build on top of existing protocols rather than replace them, their implementation necessarily depends on the structure and constraints of the integrating system.
- Suitable external yield strategies depend on protocol-specific factors such as scale, utilization patterns, governance preferences, and risk tolerance.

Conclusion

This work presents two extension-based improvements aimed at increasing capital efficiency in DeFi protocols: one by reallocating idle lending-pool capital into external yield sources, and the other by preserving productive concentrated liquidity under directional price drift.